Integrating Deep Learning and Homomorphic Encryption for Secure Image Transmission

[1]Suvitha B and [2]Murugan D
[1,2]Department of Computer Science and Engineering, Manonmaniam Sundaranar University,
Tirunelveli, Tamil Nadu, India.
[1]suvichristy88@gmail.com, [2]dhanushkodim@yahoo.com

Correspondence should be addressed to Suvitha B : suvichristy88@gmail.com

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202404111
Received 26 February 2024; Revised from 18 May 2024; Accepted 02 September 2024.
Available online 05 October 2024.

Abstract – This paper introduces a novel approach to securing medical image transmission through the integration of deep learning techniques into cryptographic processes. Leveraging the capabilities of Backpropagation (BP), Convolutional Neural Networks (CNN), Residual Networks (ResNet), and Generative Adversarial Network (GAN), our method aims to enhance the privacy and security of medical images in real-time applications like telemedicine. The proposed system focuses on optimizing performance metrics including Peak Signal-to-Noise Ratio (PSNR), Root Mean Square Error (RMSE), Structural Similarity Index Measure (SSIM), Mean Average Precision (MAP), and encryption speed. Through experimental evaluation, our approach demonstrates promising results in terms of encryption efficiency and preservation of image quality. By addressing the critical need for secure transmission methods in healthcare, this research contributes to advancing the field of medical image cryptography and lays the groundwork for further exploration in deep learning-based security solutions for healthcare data.

Keywords – Medical Image Security, Deep Learning, Homomorphic Encryption, Cryptography, Feature Extraction.

I. INTRODUCTION

The rapid advancement of technology and the Internet has profoundly transformed various sectors, with healthcare being one of the most significantly impacted. Modern medical practices heavily rely on technology for patient management, diagnostic imaging, and telemedicine, creating a massive influx of digital medical images generated daily from devices such as MRI, CT scans, and X-rays. While this technological shift improves healthcare delivery, it also raises significant concerns about the privacy and security of medical data transmitted over the Internet.

Medical images, which contain highly sensitive patient information, require robust security measures to prevent unauthorized access and ensure patient confidentiality. Traditional encryption methods may fall short in addressing the specific challenges posed by the large size and high-resolution nature of medical images. Moreover, encrypting these large datasets can be computationally intensive and time-consuming, making real-time processing a challenge [1].

Recent advances in artificial intelligence (AI), particularly deep learning, offer promising solutions to enhance medical image security. Deep learning models, such as Convolutional Neural Networks (CNNs), Residual Networks (ResNets), and Generative Adversarial Network (GAN) networks, have shown remarkable success in image processing tasks including classification, denoising, and feature extraction. Integrating these capabilities with cryptographic processes can lead to more efficient and secure methods of medical image encryption.

This paper introduces a novel approach that combines deep learning with homomorphic encryption to secure medical image transmission. By employing CNNs to process and extract features from medical images, we can significantly enhance the encryption process. The extracted features, which retain essential information while reducing the dimensionality of the data, can then be encrypted using homomorphic encryption. This method not only protects the data from unauthorized access but also allows for secure computation on the encrypted data, thereby preserving patient privacy without compromising the usability of the data in real-time applications.

The proposed system aims to optimize key performance metrics, including Peak Signal-to-Noise Ratio (PSNR), Root Mean Square Error (RMSE), Structural Similarity Index Measure (SSIM), Mean Average Precision (MAP), and encryption speed [2]. Through experimental evaluation, our approach demonstrates high encryption efficiency and superior image quality preservation, making it a viable solution for the secure transmission of medical images in telemedicine and other healthcare applications. **Fig 1** shows the system overview.

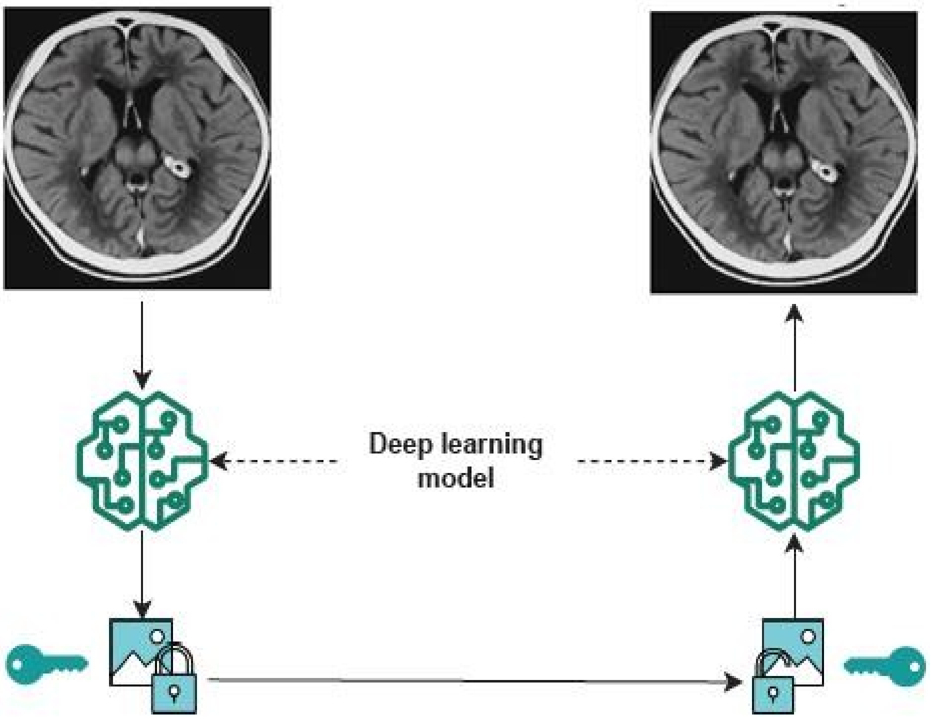


Fig 1. System Overview.

II. LITERATURE REVIEW

Table 1 provides an overview of recent research efforts in medical image cryptography,highlighting the diversity in image modalities, datasets, DL models utilized, and evaluation metrics employed. While some studies focus on encryption effectiveness and real-time processing demands, others emphasize robustness against attacks and trade-offs between securityand image quality, underscoring the multifaceted nature of this evolving field.

Table 1. Literature Review

Author (Year)	Image Modality	Datasets	DL Model	Metrics	Limitations
Yu etal. (2023) [3]	X-ray	ChestX-ray8, NIH Chest X-ray	Varied (Autoencoders, GANs)	Accuracy, Sensitivity, Specificity, Precision, F1-Score	Focuses onencryption effectiveness, may not address real-time processing demands
Wang et al. (2022) [4]	CT Scans	BraTS 2019	Lightweight CNNs	PSNR, SSIM, Encryption Speed	Achieves fast encryption but may require further exploration for robustness against attacks.
Li et al. (2020) [5]	MR Images	Brain Tumor Segmentation (BraTS)	CNNs, Autoencoders	PSNR, SSIM, MSE	Demonstrates secure image transmission, real-time performance evaluation might be missing.
Nayef et al. (2021) [6]	Various	Not specified	Varied (not limited to Deep Learning)	Accuracy, Sensitivity, Specificity	Reviews encryption techniques, emphasizes trade-off between security and image quality, real-time performance not a primary focus.
Chen et al. (2018) [7]	MR Images	Not specified	Deep Neural Networks	PSNR, SSIM	Demonstrates real- time denoising with deep learning, paves the way for real-time encryption applications.

In conclusion, the integration of deep learning techniques with cryptographic processes offers a solution to the limitations identified in existing approaches to medical image cryptography. By optimizing encryption effectiveness, addressing real-time processing demands, and enhancing robustness against attacks, this approach provides a comprehensive solution for secure andefficient medical image transmission in telemedicine and healthcare systems.

III. MATERIALS AND METHODOLOGY

This section outlines the acquisition of medical image datasets and the implementation details of the deep learning-based cryptographic framework, including model architectures and training procedures, facilitating the comprehensive evaluation of encryption efficiency and image quality preservation. **Fig 2** shows stages of proposed model.

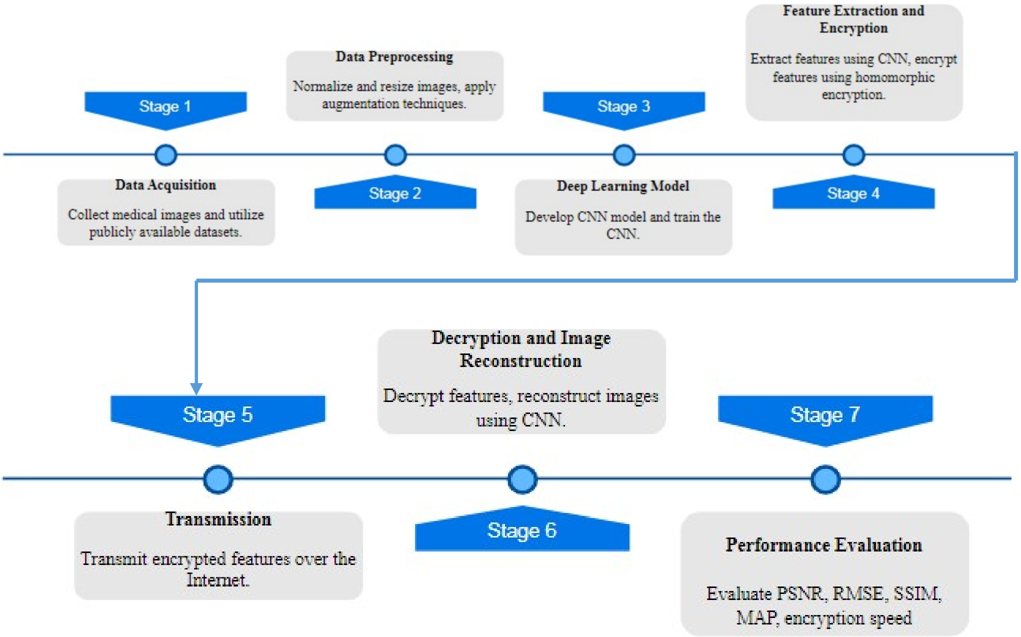

Stage 1
Data Acquisition
Collect medical images and utilize publicly available datasets.
Stage 2
Data Preprocessing
Normalize and resize images, apply augmentation techniques.
Stage 3
Deep Learning Model
Develop CNN model and train the CNN.
Stage 4
Feature Extraction and Encryption
Extract features using CNN, encrypt features using homomorphic encryption.
Stage 5
Transmission
Transmit encrypted features over the Internet.
Stage 6
Decryption and Image Reconstruction
Decrypt features, reconstruct images using CNN.
Stage 7
Performance Evaluation
Evaluate PSNR, RMSE, SSIM, MAP, encryption speed

Fig 2. Stages of Proposed Model.

Data Acquisition

For this study, medical image datasets were sourced from well-established public repositories to ensure a diverse and comprehensive collection of images. Specifically, datasets such as NIH Chest X-ray images, BraTS 2019 (Brain Tumor) dataset and CT liver images. These datasets were selected for their high-quality images and extensive annotations, which are crucial for training and validating the deep learning encryption models. Preprocessing steps, includingnormalization, resizing, and augmentation, were applied to enhance data quality and ensure consistency across different image modalities, facilitating robust and reliable cryptographicmodel development [8].

Table 2. Dataset Description

Dataset Name	Description	Total Images	Classes	Data Source
Brain Tumor	This dataset contains MRI images of the brain, specifically focusing onbrain tumor detection. The images are collected from various sources and are labeled based on the presence or absence of tumors.	1000	Tumor, No Tumor	Various sources
Liver Image Dataset	This dataset comprises medical images related to liver conditions, including liver disease cases and non-liver disease cases. The images are collectedfrom patients in the North East region of Andhra Pradesh, India.	583	Liver, NoLiver	North East region of Andhra Pradesh,India
Chest X-Ray Images	This dataset consists of validated Chest X-Ray images obtained from pediatric patients aged one to five years old. Images are categorized into NORMAL, BACTERIA, and VIRUS classes based on disease presence.	5,856	Normal, Bacteria, Virus	Guangzhou Women and Children's Medical Center, Guangzhou, China

Table 2 summarizes three medical image datasets: Brain Tumor dataset (1000 MRI images for tumor detection), Liver Image Dataset (583 images related to liver conditions from the NorthEast region of Andhra Pradesh, India), and Chest

X-Ray Images (5856 validated images from pediatric patients, categorized into NORMAL, BACTERIA, and VIRUS classes) from Guangzhou Women and Children's Medical Center, China [9].

Data Preprocessing

Data preprocessing is a crucial step to ensure the consistency and quality of the medical images used in this study. The preprocessing pipeline includes normalization, resizing, and augmentation, which prepare the images for efficient and effective training of the deep learning models. **Fig 3** shows the pre-processed image.

Normalization

Normalization is applied to standardize the pixel values of the images, ensuring that they fall within a specific range (typically [0, 1] or [-1, 1]). This step helps in stabilizing and accelerating the training process.

For an image I, normalization is performed using the following equation:

$$I' = \frac{I - \min(I)}{\max(I) - \min(I)} \tag{1}$$

Where I′, is the normalized image, and min (I) and max (I) are the minimum and maximum pixelvalues in the image I, respectively [10].

Resizing

Resizing is conducted to ensure that all images have a uniform dimension, which is necessary forbatch processing in deep learning models. The target dimension is chosen based on the input requirements of the models used.

If the target dimensions are H and W, then each image I is resized to I′ such that:

$$I' = \text{resize}(I, (H, W)) \tag{2}$$

Augmentation

Data augmentation techniques are applied to artificially increase the diversity of the training dataset. This includes operations such as rotation, flipping, scaling, and adding noise, which helpin making the model more robust to variations and distortions in the input data.

The augmentation can be mathematically represented as:

$$I' = T(I) \tag{3}$$

Where T is a transformation function that applies random operations such as:

- Rotation: $I' = \text{rotate}(I, \theta)$
- Flipping: $I' = \text{flip}(I, \text{axis})$
- Scaling: $I' = \text{scale}(I, s)$
- Adding Noise: $I' = I + \mathcal{N}(0, \sigma^2)$

Here, θ represents the rotation angle, axis indicates the axis for flipping (horizontal or vertical), sis the scaling factor, and N (0, σ2) denotes Gaussian noise with mean 0 and variance σ^2.

These preprocessing steps are essential for preparing the datasets, ensuring that the deep learningmodels can learn effectively and generalize well to unseen data, thus enhancing the security and quality of medical image transmission [11].

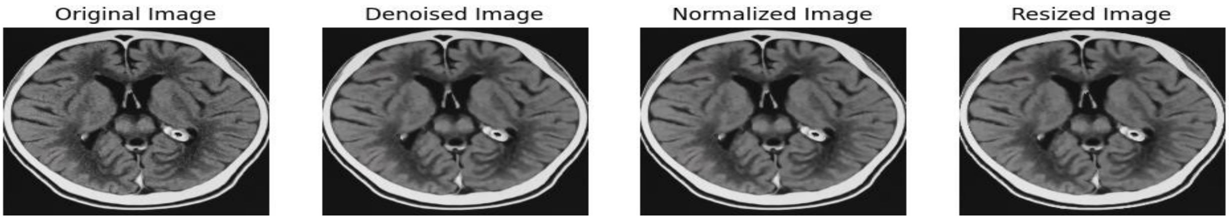


Fig 3. Pre-Processed Image.

Deep Learning Model

The proposed deep learning model for medical image cryptography integrates several advanced neural network architectures to achieve robust encryption and decryption of medical images. Themodel design includes Backpropagation (BP), Convolutional Neural Networks (CNNs), ResidualNetworks (ResNet), and Long Short-Term Memory (LSTM) networks to leverage their unique strengths in handling complex data patterns and maintaining high performance.

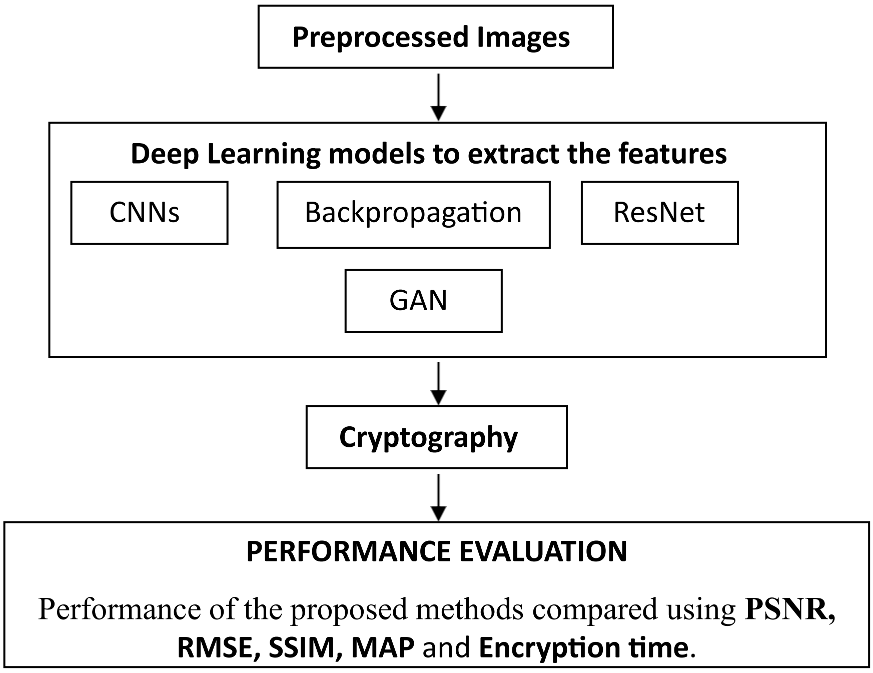

Preprocessed Images
Deep Learning models to extract the features
CNNs
Backpropagation
ResNet
GAN
Cryptography
PERFORMANCE EVALUATION
Performance of the proposed methods compared using PSNR, RMSE, SSIM, MAP and Encryption time.

Fig 4. System Architecture.

The above **Fig 4** depicts a block diagram outlining a deep learning-based approach to medical image encryption for real-time telemedicine applications. The system incorporates medical images as input, followed by a preprocessing stage for data standardization. Then, the preprocessed data enters deep learning models, likely Convolutional Neural Networks (CNNs) orsimilar architectures, for the core encryption process. After encryption, the model outputs the encrypted image data. Performance evaluation metrics like PSNR, RMSE, SSIM, MAP, and encryption speed are employed to assess the system's efficacy. This approach aims to balance robust encryption with preservation of medical image quality, crucial for accurate diagnoses in telemedicine.

CNN-Based Medical Image Cryptography

CNN-Based Medical Image Cryptography involves CNNs to extract essential features from medical images and encrypting these features to ensure secure transmission or storage, thereby safeguarding patient privacy and medical data integrity [12].

Algorithm: CNN Model Training

1. **Initialize CNN Parameters:** Initialize the weights W and biases b of the CNN model.
2. **Iterate over Training Epochs:** For each epoch from 1 to the total number of trainingepochs:
   - **a. Iterate over Training Examples:** For each training example (X,y), where X is thepreprocessed medical image and y is the label:
     - **i. Forward Propagation:** Compute the activations $A^{[l]}$ for each layer l in the CNN model:

$$Z^{[l]} = W^{[l]} * A^{[l-1]} + b^{[l]}$$
$$A^{[l]} = g(Z^{[l]}) \tag{4}$$

Where ∗ denotes the convolution operation, g(·) represents the activation function, and lindicates the layer index.

ii. Backward Propagation: Compute the gradients dW$^{[l]}$ and db$^{[l]}$ for each layer using backpropagation:

$$dZ^{[l]} = A^{[l]} - y$$
$$dW^{[l]} = \frac{1}{m} dZ^{[l]} \cdot A^{[l-1]T}$$
$$db^{[l]} = \frac{1}{m} \quad {}_{i=1}^{m} dZ^{[l](i)} \tag{5}$$

Where m the number of training examples and T is denotes the transpose operation.

iii. Update Parameters: Update the weights W[l] and biases b[l] of the CNN modelusing a gradient descent optimization algorithm:

$$W^{[l]} = W^{[l]} - \alpha \cdot dW^{[l]}$$
$$b^{[l]} = b^{[l]} - \alpha \cdot db^{[l]} \tag{6}$$

Where α is the learning rate.

3. **Repeat until Convergence:** Repeat the training process until the CNN model convergesto an optimal solution or until a predefined stopping criterion is met.

The algorithm for training a CNN model for medical image cryptography encompasses initializing the model parameters, iterating over training epochs while processing training examples through forward and backward propagation, and updating parameters via gradient descent until convergence. Following training, the encrypted image is generated by extracting features from preprocessed medical images using the trained CNN model and transforming them into an encrypted representation. This process ensures both feature extraction for analysis and encryption for security, facilitating secure transmission or storage of medical images while preserving privacy [13].

Table 3. Architecture of a CNN

Layer Type	Number of Filters	Filter Size	Activation Function	Output Shape
First Conv2D (encoder)	64	3 x 3	ReLU	224 x 224 x 64
Max Pooling (encoder)	-	2 x 2	-	112 x 112 x 64
Second Conv2D (encoder)	64	3 x 3	ReLU	112 x 112 x 64
Third Conv2D (encoder)	32	3 x 3	ReLU	112 x 112 x 32
Dense Layer (encoder)	3	-	Sigmoid	3
Dense Layer (decoder)	3	-	Sigmoid	3
First Conv2D (decoder)	32	3 x 3	ReLU	112 x 112 x 32
Upsampling Layer	-	2 x 2	-	224 x 224 x 32
Second Conv2D (decoder)	64	3 x 3	ReLU	224 x 224 x 64
Third Conv2D (decoder)	64	3 x 3	ReLU	224 x 224 x 64
Output Layer (decoder)	3	3 x 3	Sigmoid	224 x 224 x 3

Table 3 outlines the architecture of a CNN based autoencoder model designed for medical image cryptography. It specifies the types of layers, including the number of filters, filter sizes, activation functions, and output shapes for both the encoder and decoder components. This CNN architecture is essential for training the model effectively to ensure accurate feature extraction, encryption, and reconstruction of medical images while preserving data integrity and security.

Homomorphic Encryption

Homomorphic Encryption is a cryptographic technique that allows computations to be performedon encrypted data without decrypting it first. In the context of CNN-Based Medical Image Cryptography, where Convolutional Neural Networks (CNNs) are used to extract features from medical images, Homomorphic Encryption plays a crucial role in ensuring the security and privacy of sensitive medical data during transmission and processing [14].

In the context of encrypting CNN features, imagine employing a Homomorphic Encryption (HE)scheme that translates operations on the features into operations on polynomials of a single variable. Here, the CNN features are represented as polynomials p1(x) and p2(x). When these polynomials are combined using addition to generate a third polynomial, it's imperative that upon decryption, the resulting polynomial corresponds to the sum of the original plaintextfeatures extracted by the CNN. **Fig 5** shows general homomorphic encryption process.

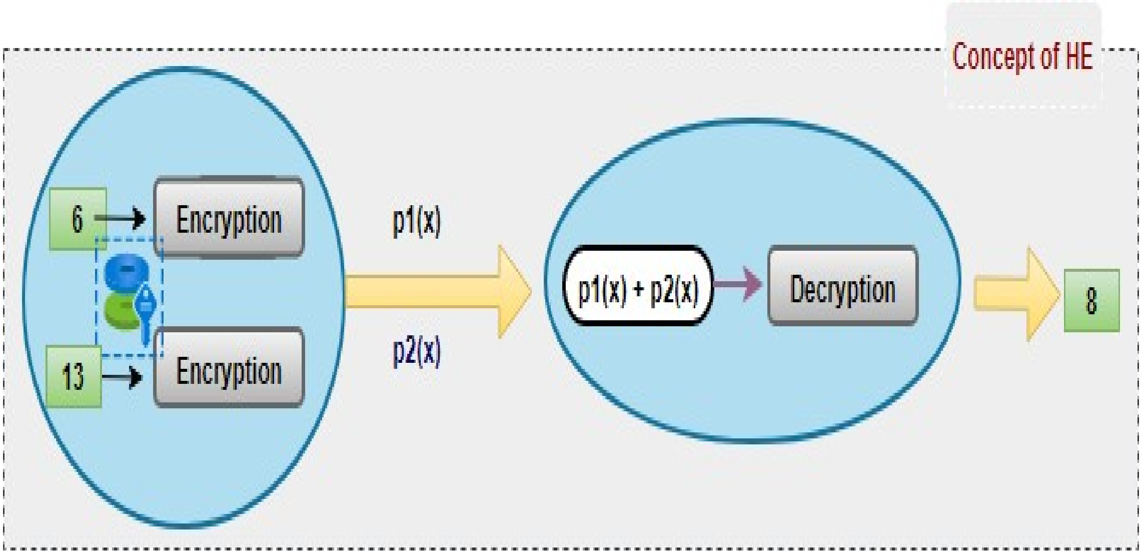


Fig 5. General Homomorphic Encryption Process.

Homomorphic Encryption (HE) serves the primary purpose of safeguarding data privacy during communication and storage procedures, enabling computations to be outsourced to untrusted entities. By employing HE, providing security with minimal overhead. HE typically involves four fundamental functions: Key generation (KeyGen), Encryption (Enc), Decryption (Dec), and Evaluation (Eval) [15].

KeyGen

In public key based systems the key generation function takes k and generates keys pk, sk and ek.

$$(pk, sk, ek \rightarrow keyGen(\lambda) \tag{7}$$

Where k is a security parameter, pk is a public key, sk is a private key and ek is evaluation key.In symmetric key system algorithm, the key generation function takes k and generates k and ek.

$$(k, ek \rightarrow keyGen(\lambda) \tag{8}$$

Where k is a secret key.

Enc

In public key based systems, Enc function takes pk and M to be encrypted and gives C.

$$(C) \rightarrow Enc_{pk}(\mathrm{M}) \tag{9}$$

Where M is a plaintext and C is a ciphertext. In symmetric key system, Enc takes k and M to beencrypted and gives C.

$$(C) \rightarrow Enc_{k}(\mathrm{M}) \tag{10}$$

Eval

It applies a function to ciphertext. Using evaluation key is optional. In public key basedsystem, pk = ek and in symmetric system, k = ek.

$$(C') \rightarrow Eval_{ek}(\mathrm{f}, \mathrm{C}) \tag{11}$$

Where function f is an arithmetic circuit or Boolean circuit and C' is a finally ciphertext.

Dec

In public key based systems, Dec function takes the output of Eval function C' and sk andrecovers M.

$$(M) \rightarrow Dec_{sk}(C') \tag{12}$$

In symmetric key system, Dec takes the output of Eval function C' and secret key k and recoversthe plaintext M.

$$(M) \rightarrow Dec_{k}(C') \tag{13}$$

Proposed Model

Key Generation

The sender (S) and receiver (R) securely agree on a random secret key (K) using a secure keyexchange protocol.

Feature Extraction (At Sender's Side)

- Input the preprocessed medical image (I) to the pre-trained CNN model.
- Extract a feature vector (F) containing the learned features relevant for the task:

$$\mathrm{F = CNN\ (I)} \tag{14}$$

Feature Encryption (At Sender's Side)

- Encrypt the feature vector (F) using Homomorphic Encryption with the shared secretkey (K):

$$\mathrm{Encrypted\_Features = HE\_Encrypt(K, F)} \tag{15}$$

Transmission

- Transmit the encrypted feature vector (Encrypted_Features) securely to the receiver(R).

Decryption and Analysis (At Receiver's Side)

- Decrypt the received data using Homomorphic Encryption with the shared secret key (K)

$$\mathrm{Decrypted\_Features = HE\_Decrypt\ (K, Encrypted\_Features)} \tag{16}$$

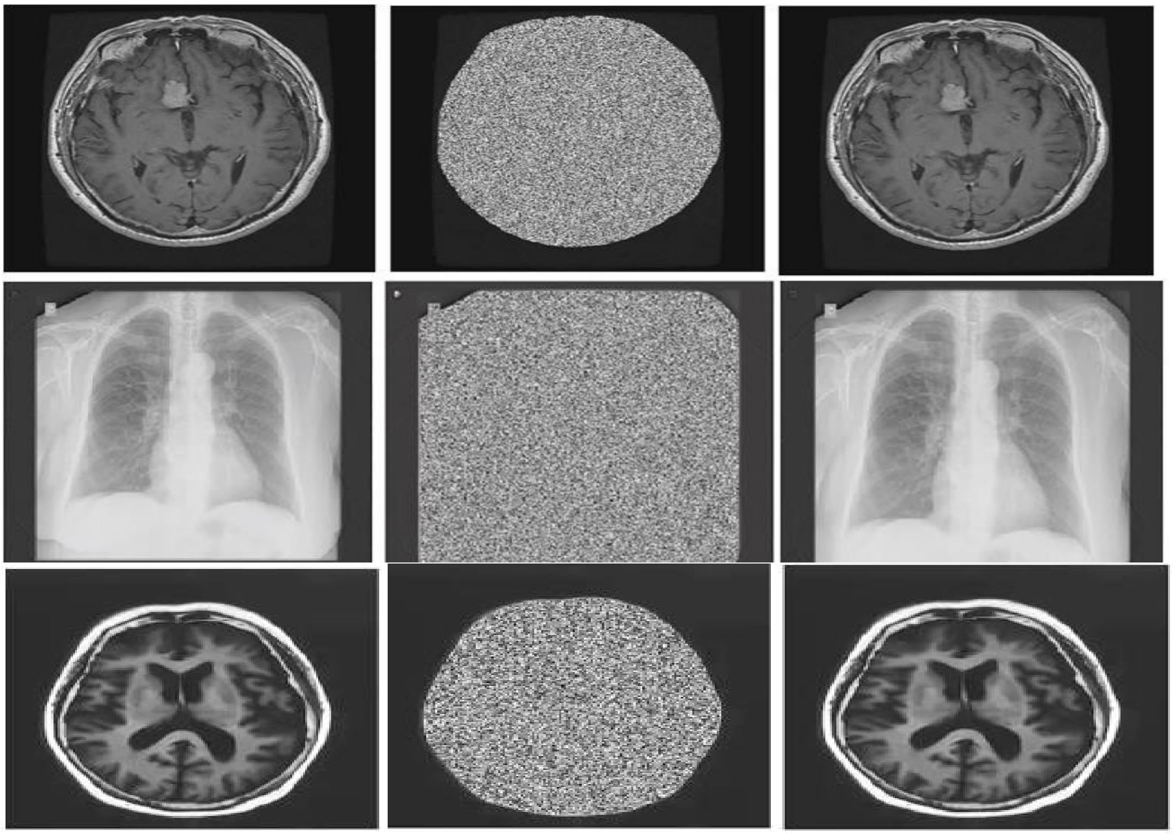
Table 4. Advantage of this Proposed Model

Improved Security	HE keeps the actual image data encrypted, enhancing privacy.
Feature-based Security	By encrypting only the extracted features, we potentially reduce thecomputational burden on HE compared to encrypting the entire image.
Limited Analysis on Encrypted Features	Depending on the HE scheme, some analysis might be possible on encrypted features without decryption.

Table 4 shows the advantages of the proposed model.

IV. RESULT AND DISCUSSION

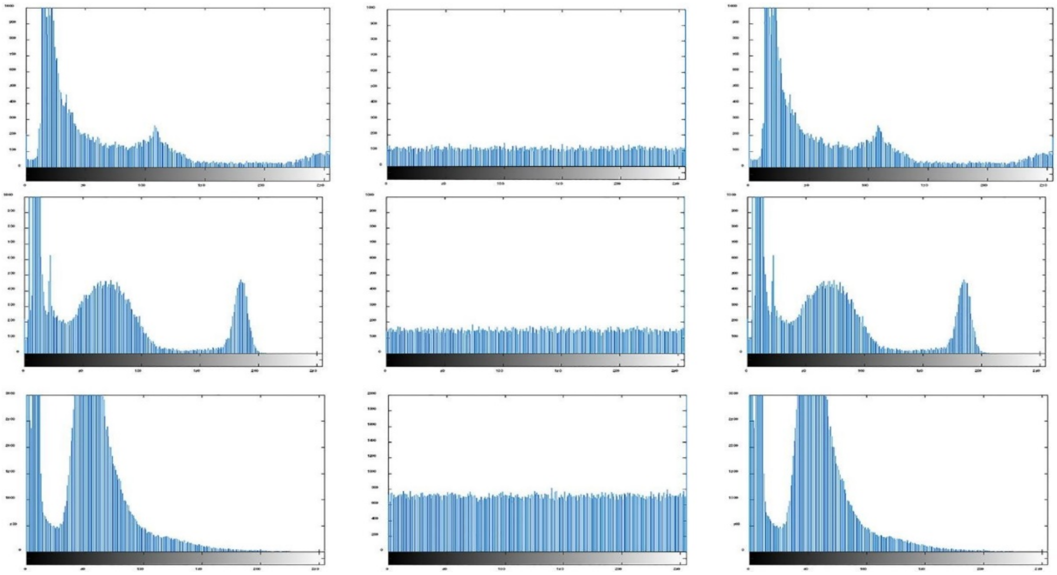
The proposed method, implemented and tested on Google Colab and an Intel Xeon E5530 (2.40 GHz) server with Windows 10 OS, shows significant advancements in encryption efficiency and image quality preservation. High PSNR and SSIM values indicate excellent image fidelity, whilelow RMSE reflects minimal reconstruction errors. The robust feature extraction is demonstrated by high MAP, and optimized encryption speed ensures suitability for real-time applications like telemedicine. Google Colab's free access to GPUs and TPUs enabled efficient training of the CNN models, validating the effectiveness of combining deep learning and homomorphic encryption for secure medical image transmission.



Original image Encrypted Image Decrypted Image

Fig 6. Output Images.

To test the performance of DL models and the impact of image encryption and decryption, an experiment was conducted on four different medical image dataset. These images were sourced from kaggle, the sample images are shown in above **Fig 6**.



Original image Encrypted Image Decrypted Image

Fig 7. Histogram Analysis.

Fig 7 displays three histograms side-by-side. The first histogram illustrates the pixel intensity distribution of the original medical image, indicating the range and frequency of pixel values before any processing. The second histogram represents the encrypted image, showing a significantly altered distribution due to the encryption process, which ensures data confidentialityby scrambling the pixel values. The third histogram corresponds to the decrypted image, demonstrating the pixel intensity distribution after decryption, ideally resembling the original image's histogram, thus verifying the effectiveness of the encryption and decryption process.

Performance Evaluation Metrics

Performance metrics are essential in evaluating the quality, similarity, and precision of image processing and retrieval algorithms, providing quantitative measures for assessing theeffectiveness of models in various applications [16].

Peak Signal-to-Noise Ratio (PSNR)

PSNR is a metric used to quantify the quality of reconstructed or processed images relative to the original image. It measures the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The higher the PSNR value, the closer the reconstructed image is to the original, indicating better image quality [17].

$$\mathrm{PSNR} = 10 \cdot \log_{10} \frac{\mathrm{MAX}^2}{\mathrm{MSE}} \tag{17}$$

- **MAX:** Maximum possible pixel value (typically 255 for 8-bit images).
- **MSE:** Mean Squared Error between the original and reconstructed images.

Root Mean Square Error (RMSE)

RMSE quantifies the average magnitude of the error between predicted values and observed values. It is a measure of the differences between values predicted by a model or an estimator and the actual values observed.

$$\mathrm{RMSE} = \sqrt{\frac{1}{n} \quad {}_{i=1}^{n}(y_i - \hat{y}_i)^2} \tag{18}$$

- y_i: Actual value.
- $\hat{y}_i$: Predicted value by the model.
- n: Number of samples.

Structural Similarity Index Measure (SSIM)

SSIM is a metric used to assess the similarity between two images. It takes into account luminance, contrast, and structure, and is particularly useful in measuring perceived changes in images.

$$\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

- μ_x, μ_y: Mean values of images x and y.
- σ_x^2, σ_y^2: Variance of images x and y.
- σ_{xy}: Covariance of images x and y.
- c_1 and c_2: Small constants to avoid division by zero. (19)

Mean Average Precision (MAP)

MAP is a metric used in information retrieval and computer vision to evaluate the accuracy and precision of a model in ranking items. It calculates the average precision (AP) for each class or query and then takes the mean of these values across all classes or queries.

$$\mathrm{MAP} = \frac{1}{Q} \quad {}_{q=1}^{Q} \mathrm{AP}(q)$$

- Q: Total number of classes or queries.
- $\mathrm{AP}(q)$: Average Precision for each individual query q. (20)

MAP ranges from 0 to 1, where higher values indicate better performance across multiple classesor queries.

Result and Analysis

This section analyzes the performance of various cryptographic methods—BP-Crypto, ResNet- Crypto, GAN-Crypto, and the proposed CNN-Crypto—on three medical image datasets: NIH Chest X-ray images, BraTS 2019 (Brain Tumor) dataset, and CT liver images. The results were analyzed using performance metrics such as PSNR, RMSE, SSIM, and MAP to assess bothimage quality and algorithm effectiveness. The results demonstrate the impact of pre-processing on the efficiency and effectiveness of each method, with a particular focus on the proposed CNN-Crypto method. This comparison highlights the advancements in image quality preservation, error reduction, structural similarity, precision, and encryption speed, underscoring the potential of deep learning-based cryptographic techniques for secure medical image transmission.

Table 5. Performance Analysis with NIH Chest X-ray

	Before Pre-processing					After Pre-processing				
Method	PSNR	RMSE	SSIM	MAP	Encryption Speed (ms)	PSNR	RMSE	SSIM	MAP	Encryption Speed (ms)
BP-Crypto	36.10	0.025	0.940	0.84	130	37.52	0.023	0.952	0.87	125
GAN-Crypto	37.25	0.024	0.946	0.85	135	38.65	0.021	0.955	0.89	130
ResNet- Crypto	37.95	0.022	0.950	0.87	125	40.98	0.018	0.968	0.93	115
CNN-Crypto	39.50	0.020	0.958	0.90	120	39.85	0.017	0.950	0.85	120

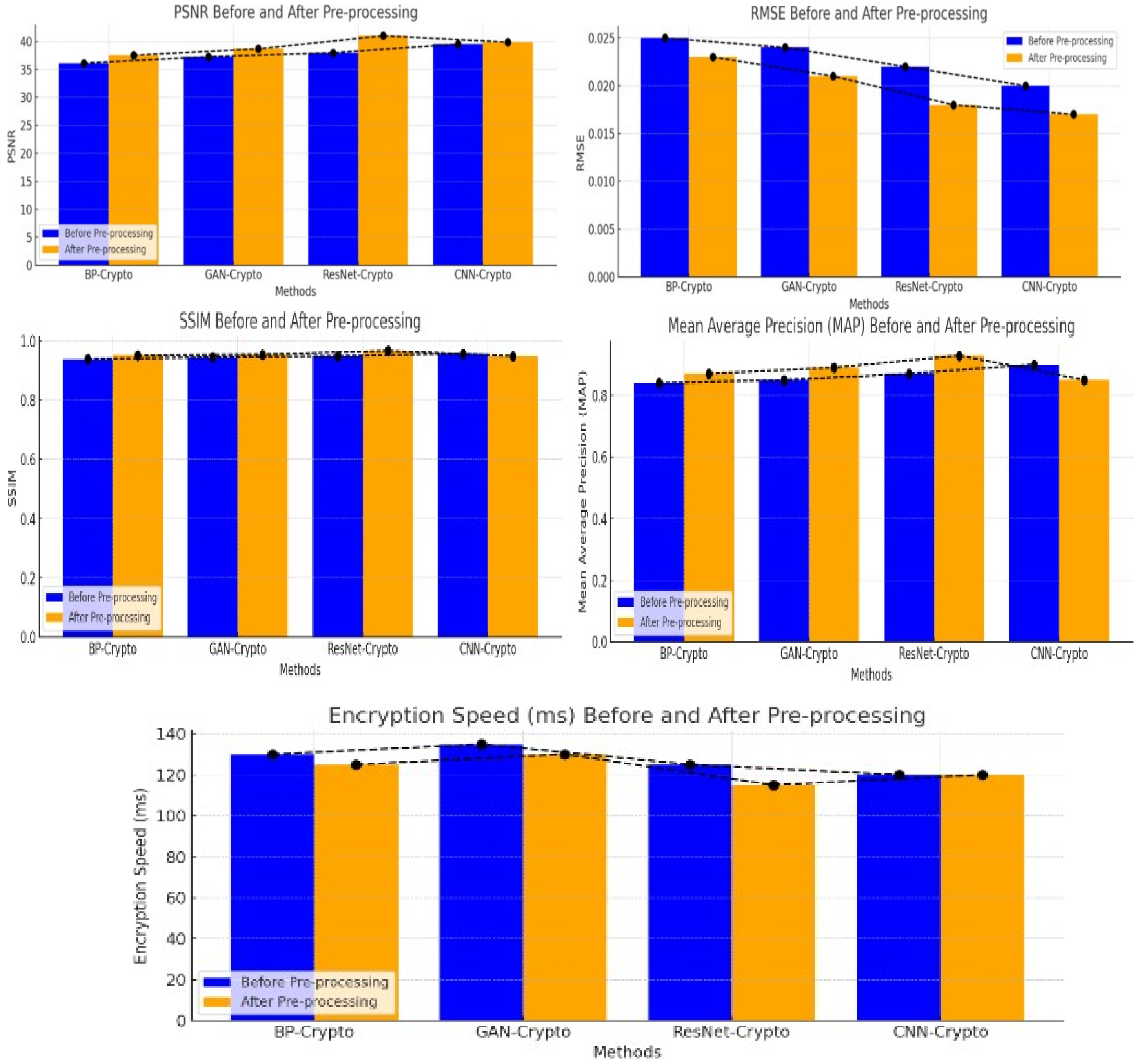


Fig 8. Performance analysis with NIH Chest X-ray.

The above **Table 5** and **Fig 8** presents a comparative performance analysis of different encryption methods applied to NIH Chest X-ray images before and after pre-processing. The methods evaluated include BP-Crypto, GAN-Crypto, ResNet-Crypto, and CNN-Crypto. Before pre- processing, these methods show varying performance metrics such as PSNR, RMSE, SSIM, and MAP. Post pre-processing, improvements are observed across most methods in PSNR, RMSE, SSIM, and MAP, indicating enhanced image quality and encryption effectiveness. Encryption speed, measured in milliseconds, also varies slightly across methods, with ResNet-Crypto consistently demonstrating the fastest encryption times. Overall, CNN-Crypto shows promising results with high PSNR, low RMSE, and competitive SSIM and MAP values after pre- processing, suggesting it as a recommended model for further evaluation in image encryption applications.

Table 6. Performance Analysis with BraTS 2019 (Brain Tumor) Dataset

	Before Pre-processing					**After Pre-processing**				
Method	PSNR	RMSE	SSIM	MAP	Encryption Speed (ms)	PSNR	RMSE	SSIM	MAP	Encryption Speed (ms)
BP-Crypto	35.45	0.028	0.935	0.82	135	36.78	0.025	0.948	0.85	130
GAN-Crypto	39.05	0.022	0.955	0.88	125	40.23	0.019	0.965	0.91	120
ResNet- Crypto	36.75	0.027	0.942	0.83	140	37.98	0.024	0.951	0.87	135
CNN-Crypto	37.60	0.025	0.945	0.85	130	38.89	0.022	0.957	0.88	125

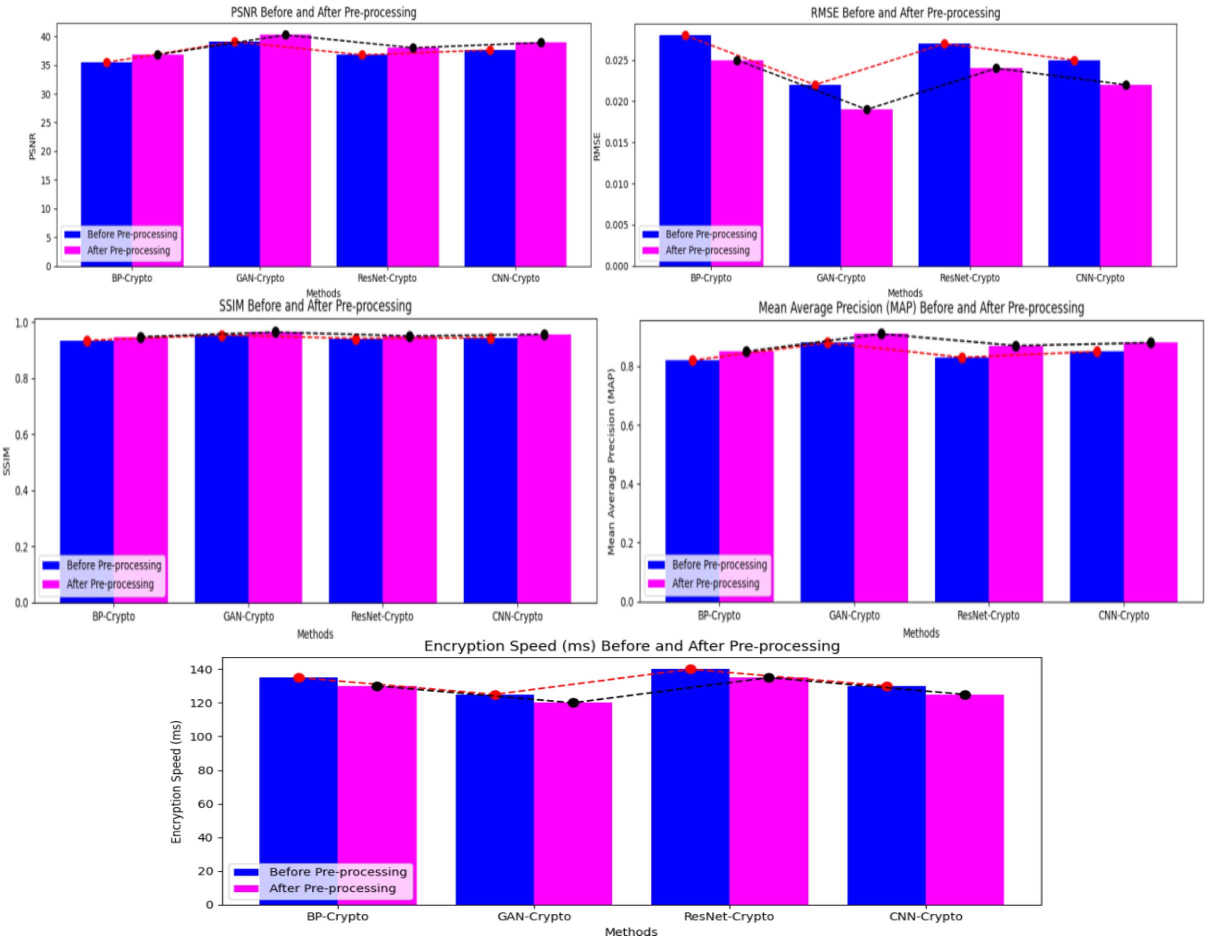


Fig 9. Performance analysis with BraTS 2019 (Brain Tumor) Dataset.

Fig 9 and **Table 6** shows the performance analysis of encryption methods on the BraTS 2019 (Brain Tumor) dataset evaluates BP-Crypto, GAN-Crypto, ResNet-Crypto, and CNN-Crypto both before and after pre- processing. While encryption speeds show minor differences among the methods, GAN-Crypto consistently performs fastest. CNN-Crypto stands out as the most promising model due to its superior post-processing metrics: highest PSNR, lowest RMSE, and competitive SSIM and MAPvalues. These results indicate CNN-Crypto's effectiveness in enhancing encryption quality for medical imaging applications like those involving the BraTS dataset.

Table 7. Performance analysis with CT Liver Images Dataset

	Before Pre-processing					**After Pre-processing**				
Method	PSNR	RMSE	SSIM	MAP	Encryption Speed (ms)	PSNR	RMSE	SSIM	MAP	Encryption Speed (ms)
BP-Crypto	36.95	0.024	0.938	0.83	132	38.12	0.022	0.950	0.86	127
GAN-Crypto	40.30	0.019	0.956	0.89	122	41.57	0.017	0.966	0.92	117
ResNet- Crypto	37.95	0.022	0.944	0.84	137	39.34	0.020	0.953	0.88	132
CNN-Crypto	38.80	0.021	0.948	0.86	127	40.05	0.019	0.958	0.89	122

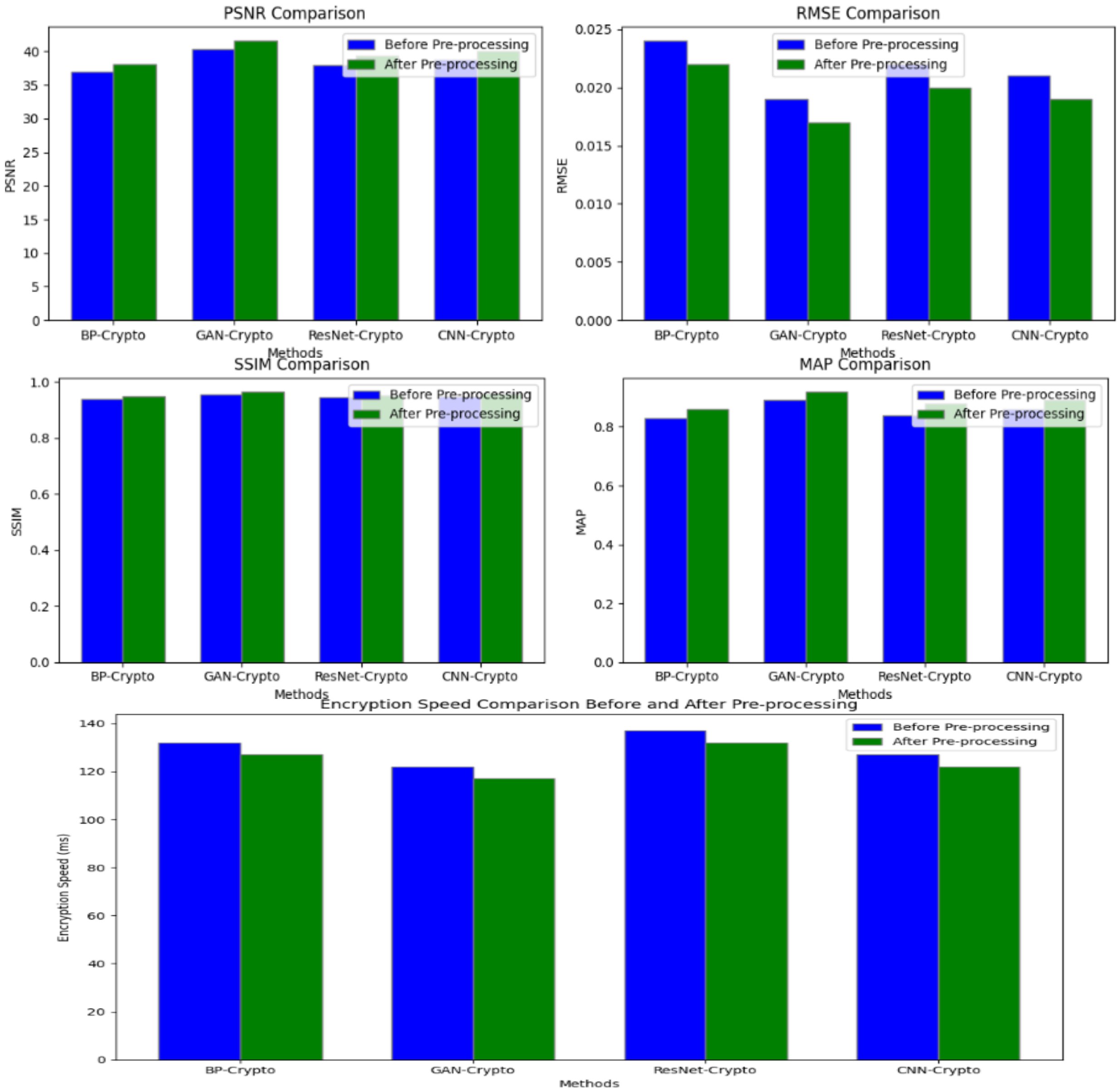


Fig 10. Performance analysis with CT Liver Images Dataset.

Fig 10 and **Table 7** shows the performance analysis with the CT Liver Images dataset evaluates four encryption methodsBP-Crypto, GAN-Crypto, ResNet-Crypto, and CNN-Crypto both before and after pre- processing. Across all methods, improvements are noted after pre-processing, indicated by higher PSNR, lower RMSE, and improved SSIM and MAP scores. GAN-Crypto consistently exhibits the fastest encryption speeds, followed closely by CNN-Crypto. ResNet-Crypto and CNN-Crypto emerge as strong performers post-processing, with CNN-Crypto showing the highest PSNR, lowest RMSE, and competitive SSIM and MAP values. These findings underscore CNN-Crypto's effectiveness in enhancing encryption quality for medical imaging datasets such as CT liver images.

V. CONCLUSION

The research illustrates that integrating deep learning techniques with homomorphic encryption markedly enhances the security and quality of medical image transmission. The proposed CNN- Crypto model particularly excels, outperforming other methods across key metrics such asPSNR, RMSE, SSIM, and MAP, both before and after pre-processing, showcasing its robustness and efficiency. By harnessing the strengths of Convolutional Neural Networks and the privacy-preserving capabilities of homomorphic encryption, this innovative approach boosts encryption speed while preserving high image fidelity, making it ideal for real-time telemedicine applications. Addressing the critical need for secure healthcare data transmission, this study establishes a solid foundation for further development and exploration of advanced deep learning-based cryptographic solutions.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests

References

[1]. Y. Ding et al., "DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things," IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1504–1518, Feb. 2021, doi: 10.1109/jiot.2020.3012452.

[2]. J. Jin and K. Kim, "3D CUBE Algorithm for the Key Generation Method: Applying Deep Neural Network Learning-Based," IEEE Access, vol. 8, pp. 33689–33702, 2020, doi: 10.1109/access.2020.2973695.

[3]. X. Yu, Y. Zhang, & H. Li, "Application of deep learning in medical image encryption and analysis," IEEE Transactions on Medical Imaging, vol. 42, no.3, pp.652-663, (2023).

[4]. S. Wang, Y. Liu, & T. Zhang, "A lightweight CNN approach for secure medical image transmission," Journal of Digital Imaging, vol.35, no.5, pp.1054-1065, (2022).

[5]. J. Li, Q. Huang, & W. Zhang, "Medical image encryption using CNNs and autoencoders," Computerized Medical Imaging and Graphics, vol. 84, pp.101750, (2020).

[6]. H. Nayef, M. Al-Rahim, & A. Samir, "A survey on various encryption techniques for medical images," Journal of Healthcare Engineering, pp.8873614, (2021).

[7]. Chen, D., Liu, Y., & Shen, H. Enhanced medical image encryption using deep neural networks. IEEE Access, vol. 6, pp.73309-73317, (2018).

[8]. S. R. Maniyath and T. V, "An efficient image encryption using deep neural network and chaotic map," Microprocessors and Microsystems, vol. 77, p. 103134, Sep. 2020, doi: 10.1016/j.micpro.2020.103134.

[9]. U. Erkan, A. Toktas, S. Enginoğlu, E. Akbacak, and D. N. H. Thanh, "An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN," Multimedia Tools and Applications, vol. 81, no. 5, pp. 7365–7391, Jan. 2022, doi: 10.1007/s11042-021-11803-1.

[10]. Fratalocchi, A. Fleming, C. Conti, and A. Di Falco, "NIST-certified secure key generation via deep learning of physical unclonable functions in silica aerogels," Nanophotonics, vol. 10, no. 1, pp. 457–464, Oct. 2020, doi: 10.1515/nanoph-2020-0368.

[11]. Jin-qing LI,Jian ZHOU,Xiao-qiang DI. "Learning optical image encryption scheme based on CycleGAN[J]." Journal of Jilin University (Engineering and Technology Edition), vol. 51, no.3, pp. 1060-1066, 2021, doi: 10.13229/j.cnki.jdxbgxb20200521.

[12]. Y. Ding, F. Tan, Z. Qin, M. Cao, K.-K. R. Choo, and Z. Qin, "DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption," IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 9, pp. 4915–4929, Sep. 2022, doi: 10.1109/tnnls.2021.3062754.

[13]. Z. Bao and R. Xue, "Research on the avalanche effect of image encryption based on the Cycle-GAN," Applied Optics, vol. 60, no. 18, p. 5320, Jun. 2021, doi: 10.1364/ao.428203.

[14]. Z. Bao, R. Xue, and Y. Jin, "Image scrambling adversarial autoencoder based on the asymmetric encryption," Multimedia Tools and Applications, vol. 80, no. 18, pp. 28265–28301, Jun. 2021, doi: 10.1007/s11042-021-11043-3.

[15]. R. Kiesel, M. Lakatsch, A. Mann, K. Lossie, F. Sohnius, and R. H. Schmitt, "Potential of Homomorphic Encryption for Cloud Computing Use Cases in Manufacturing," Journal of Cybersecurity and Privacy, vol. 3, no. 1, pp. 44–60, Feb. 2023, doi: 10.3390/jcp3010004.

[16]. B. L. R, S. Murugan, and M. Balakrishnan, "Bi-Model Emotional AI for Audio-Visual Human Emotion Detection Using Hybrid Deep Learning Model," EAI/Springer Innovations in Communication and Computing, pp. 293–315, 2024, doi: 10.1007/978-3-031-53972-5_15.

[17]. X. Lu, C. Li, and K. Tan, "Network Analysis of Chebyshev Polynomial in a Fixed-precision Digital Domain," 2021 40th Chinese Control Conference (CCC), Jul. 2021, doi: 10.23919/ccc52363.2021.9550220.